PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 9/30 — A2

(11) International Publication Number: WO 00/52877

(43) International Publication Date: 8 September 2000 (08.09.00)

(21) International Application Number: PCT/CA00/00187

(22) International Filing Date: 28 February 2000 (28.02.00)

(30) Priority Data:
2,263,056 26 February 1999 (26.02.99) CA

(71) Applicant *(for all designated States except US)*: CERTICOM CORP. [CA/CA]; 5520 Explorer Drive, 4th floor, Mississauga, Ontario L4W 5L1 (CA).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: LAMBERT, Robert [CA/CA]; 63 Holm Street, Cambridge, Ontario N3C 3N3 (CA). GALLANT, Robert [CA/CA]; 4788 Rosebush Road, Mississauga, Ontario L5M 5N1 (CA). MULLIN, Ronald [CA/CA]; 533 Twin Oaks Crescent, Waterloo, Ontario N2L 4R9 (CA). VANSTONE, Scott [CA/CA]; 539 Sandbrook Court, Waterloo, Ontario N2T 2H4 (CA).

(74) Agents: PILLAY, Kevin et al.; Orange & Chari, Suite 4900, P.O. Box 190, Toronto Dominion Bank Tower, 66 Wellington Street West, Toronto, Ontario M5K 1H6 (CA).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: METHOD AND APPARATUS FOR FINITE FIELD BASIS CONVERSION

(57) Abstract

A method and systems provided for basis conversion in a cryptographic system. The method comprises the steps of a first correspondent transmitting an element represented in the first basis to an intermediate processor, the intermediate processor converting the element into a second basis representation and forwarding the converted element to the first correspondent who then uses the converted element in a cryptographic operation. A further embodiment of the invention provides for the intermediate processor to perform the basis conversion on a field element and then forward the converted element to a second correspondent. A still further embodiment of the invention provides for the correspondents in a cryptographic scheme making use of a bit string as a function of a sequence of traces of a field element, wherein the bit string is a shared secret for performing certain cryptographic operations.